 JUDGE MOTZ

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

11 CIV 2841

JARRET AMMER, Individually, and on behalf of all others similarly situated, Plaintiffs, vs. APPLE, INC., a Delaware Corporation; PANDORA MEDIA, INC., a California Corporation; and BACKFLIP STUDIOS, INC., a Delaware Corporation; Defendants.	Civil Action No. **CLASS ACTION COMPLAINT AND DEMAND FOR JURY TRIAL**

Plaintiff, JARRET AMMER, individually and as representative of the Class defined herein (the "Class"), brings this action against the defendants identified below ("Defendants"), and avers as follows:

I. SUMMARY OF THE CASE

1. This lawsuit involves the intentional interception, by Defendants, of Plaintiff's personally identifying information ("PII"), and those belonging to members of the proposed Class. Defendants accomplish this by using iPhone and iPad mobile device applications ("Apps"). Defendants capture the devices' Unique Device ID ("UDID") – the unique identifying number that Apple, Inc. ("Apple") assigns to each of its iPhones and iPads – and transmit that information along with the devices' location data to third-party advertisers. Apple, as a joint venture with the remaining Defendants, aids and abets this intentional taking and transmitting of Plaintiff's PII and those belonging to members of the proposed Class. All of this is done without the consent of Plaintiff and members of the proposed Class and in violation of their legal rights. Plaintiff brings this lawsuit, individually and as representative of the proposed Class, to rectify this wrong being systematically perpetrated upon them.

II. PARTIES

2. Plaintiff, JARRET AMMER, is a resident of the County of Orange, State of New York. At all times relevant to this action, Plaintiff, Ammer, has owned an iPhone and had the following iPhone Apps installed on his iPhone: Pandora, and Backflip.

3. Defendant, APPLE, INC. ("Apple"), is a California Corporation with its principal place of business in Cupertino, California. Apple manufactures and sells the popular mobile phone, the iPhone, as well as the iPad.

4. Defendant, PANDORA MEDIA, INC., is a Delaware Corporation with its principal place of business at 2101 Webster Street, Ste. 1650, Oakland, California 94612. Defendant, Pandora, is the maker of the iPhone App, Pandora.

5. Defendant, BACKFLIP STUDIOS, INC., is a Delaware Corporation with its principal place of business in Boulder, Colorado. Defendant, Backflip Studios Inc., is the maker of the iPhone App, Paper Toss.

III. JURISDICTION AND VENUE

6. This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1332(d), because at least one member of the class is a citizen of a different State than the Defendants, there are 100 or more class members and the aggregate amount in controversy exceeds $5,000,000, exclusive of interest and cost. This Court also has jurisdiction pursuant to 28 U.S.C. §1331 (federal question jurisdiction), as it involves allegations of violation of federal law. This Court has pendent jurisdiction of all alleged state law claims.

7. Venue is appropriate in this District because Defendant Apple, as well as certain members of the proposed class, is a resident of this District and Defendants have committed torts within the Southern District of New York.

8. Each of the Defendants in this action, other than Defendant Apple, sells or provides its mobile device application ("Apps") to any iPhone and iPad user who wishes to download them from the iTunes App Store. Each Defendant, other than Apple, has thus marketed and sold its product within the State of New York and, upon information and belief, has sold or provided its products to millions of New York State residents. Furthermore, each non-New York Defendant has contracted with a New York State company, Defendant Apple, to sell products on a nationwide basis. Defendant Apple is a resident of the State of New York and is a resident of this District.

9. Thus, for those Defendants not residing within the State of New York, there exist sufficient minimum contacts with the State of New York, such that hailing them to answer for their violations of Plaintiff'slegal rights, and those belonging to members of the proposed Class, in the State of New York does not offend traditional notions of fair play and substantial justice.

IV. STATEMENT OF FACTS

11. This is a consumer Class Action lawsuit pursuant to Federal Rules of Civil Procedure 23(a), (b)(1), (b)(2), and (b)(3).

12. The basis for claims made by Plaintiff and members of the proposed Class rest on Defendants' use of an intrusive tracking scheme implemented through the use of mobile device Apps on iPhones and iPads belonging to Plaintiff and members of the proposed Class.

13. Apps are computer programs that users can download and install on their mobile computer devices, including iPhones and iPads.

14. While Apps have been available for some time, it was with the introduction of Apple's iPhone in 2007 that Apps propelled themselves into a position of prominence in the daily lives of many mobile device users.

15. With features more like a laptop than a mobile phone, the iPhone enabled millions of mobile phone users to more effectively and more intuitively access the Internet and perform the computer functions that have become increasingly important in today's world. In addition, the iPhone features numerous games and other forms of entertainment for its users.

16. Unlike most earlier mobile phones, the iPhone allows users to install after-market programs, called Apps, onto their mobile device. This allows users, such as Plaintiff and members of the proposed Class, to customize their iPhones to perform functions other than those that the phones could perform when they were initially sold to the consumers.

17. Numerous other mobile device manufacturers have followed Apple's lead in allowing the installation of Apps on their users' mobile devices.

18. From the beginning, Apple has retained significant control over the software that users can place on their iPhones. Apple claims that this control is necessary to ensure smooth functioning of the iPhone. For instance, iPhone users are only allowed to download software specifically licensed by Apple. If a user installs any software not approved by Apple, the users' warranty is voided. If the user updates the operating system on their iPhone, the non-licensed software is erased by Apple.

19. Apple also retains a significant amount of control over the types of Apps it allows into its newly created market place. Whether an App is allowed to be sold in the App Store is completely at the discretion of Apple. Apple requires that proposed Apps go through a rigorous approval process. Even if an App meets the "Program" requirements (as Apple describes it) the App can still be rejected by Apple for any reason at all. It is estimated that approximately twenty

percent (20%) of all requests to place Apps for sale in the iTunes App Store are rejected by Apple. In exchange for Apple agreeing to allow the App developer to participate in its "Program," Apple retains thirty percent (30%) of all revenues from sales of the App.

20. Apple also exercises a significant amount of control over the functionality of the Apps that it allows into its "Program." For instance, Apple restricts how Apps interact with the iPhone's operating system and restricts Apps from disabling certain safety features of the iPhone.

21. Despite Apple's restrictions, Apple's App Store has been a huge success. As of October 20, 2010, there were at least 300,000 third-party applications officially available on the App Store, with over seven (7) billion total downloads. Market researcher, Gartner Inc., estimates that world-wide App sales this year will total $6.7 billion.

22. Apple's iPhone has also succeeded in helping to bring hand-held computing to the masses. Approximately fifty-nine (59) million people now have an iPhone. With the subsequent introduction of its iPad (estimated sales of 8.5 million in 2010), Apple has obtained a remarkable reach for its products.

23. Thanks in part to the iPhone's tremendous commercial success, mobile devices (including iPhones and iPads) are now used by many consumers in almost all facets of their daily lives, from choosing a restaurant, to making travel arrangements, to conducting bank transactions. Most consumers carry their mobile devices with them everywhere they go. While this convenience is valuable to consumers, so is the information that consumers put into their mobile devices.

24. Because Apps are software that users, such as Plaintiff and members of the proposed Class, download and install on their iPhone (which is a hand-held computer), Apps have access to a huge amount of information about a mobile device user. Apps can have access

to such items as a mobile device's contacts list, username and password, and perhaps most importantly—the user's location information. Plaintiff and members of the proposed Class in this action consider the information on their phone to be personal and private information.

25. All of this information, however, is of extreme interest to many advertising networks. This information is also highly valuable. It is for this reason that many Apps are given away for free by the developer—just so that the App developer can sell advertising space on its App. Some advertising networks pay App developers to place banner ads within their Apps. Those ads are then populated with content from the third-party advertising network. In the process, those third-party advertisers are able to access various pieces of information from the user's iPhone, supposedly in order to serve ads to the App user that are more likely to be of interest to them.

26. Considering that mobile advertising is projected to be $1.5 billion a year industry by 2016, advertisers, website publishers, and ad networks are seeking ways to better track their web users and find out more about them. The ultimate goal of many advertising networks is to ascertain the identity of particular users so that advertisements can be tailored to their specific likes and dislikes.

27. Browser cookies are the traditional method used by advertisers to track web users' activities. But browser cookies have a large hurdle when it comes to an advertiser's ability to track a viewer because users often delete them because they do not want advertising companies to have information about them.

28. Defendants, however, have found their solution – the Unique Device ID ("UDID") that Apple assigns to every iPhone and iPad it manufactures. Apple's UDID is an example of a computing device ID generally known as a global unique identifier ("GUID"). A

GUID is a string of electronically readable characters and/or numbers that is stored in a particular device or file (*e.g.*, piece of hardware, copy of software, database, user account) for purposes of subsequently identifying the device or file. Thus, a GUID is similar to a serial number in that it is so unique that it reliably distinguishes the particular device, software copy, file, or database from others, regardless of the operating environment.

29. Because the UDID is unique to each iPhone and iPad, it is an attractive feature for third-party advertisers looking for a means of reliably tracking a mobile device users' online activities. Because the UDID is not alterable or deletable by a iPhone or iPad user, some have referred to the UDID as a "supercookie." While not technically correct (because the UDID is on the device from the time of its manufacturing), this description aptly summarizes the desirability of access to the UDID from an advertising perspective.

30. Apple's UDID is concerning for several reasons. First, unlike with desktop computers, mobile devices travel most everywhere with the user. Also, mobile devices tend to be unique to an individual. While someone might borrow someone's mobile device briefly, it is unusual for individuals to frequently trade mobile devices with someone they know.

31. Furthermore, unlike a desktop computer, the iPhone and iPad come equipped with the tools necessary to determine their geographic location. Thus, being able to identify a unique device, and combining that information with the devices' geographic location, gives the advertiser a huge amount of information about the user of a mobile device. From the perspective of advertisers engaged in surreptitious tracking, this is a perfect means of tracking mobile device users' interests and likes on the Internet.

32. Apple certainly understands the significance of its UDID and users' privacy, as, internally, Apple claims that it treats UDID information as "personally identifiable information" because, if combined with other information, it can be used to personally identify a user.

33. Unfortunately, however, unlike with browser cookies, Apple does not provide users any way to delete or restrict access to their devices' UDIDs. Traditional efforts to prevent Internet tracking, such as deleting cookies, have no effect on Apps' access to an iPhone's or iPad's UDID.

34. Apple has, however, recognized that it could go further to protect its users' private information from being shared with third parties. Thus, in April of 2010, Apple amended its Developer Agreement purporting to ban Apps from sending data to third-parties except for information directly necessary for the functionality of the App. Apple's revised Developer Agreement provides that "the use of third party software in Your Application to collect and send Device Data to a third party for processing or analysis is expressly prohibited."

35. This change prompted a number of third-party advertising networks (who have been receiving a steady flow of user data from iPhone and iPad Apps) to protest. One prominent critic was the CEO of AdMob. It appears that, as a result of this criticism, Apple has taken no steps to actually implement its changed Developer Agreement or enforce it in any meaningful way.

36. In this lawsuit, each of the non-Apple Defendants, through the use of Apps placed on mobile devices belonging to Plaintiff and members of the proposed Class, accessed UDID and location information of Plaintiff and members of the proposed Class and transmitted that information to numerous third-party ad networks.

37. The general practice engaged in by Defendants was recently confirmed by Eric Smith, Assistant Director of Information Security and Networking at Bucknell University in Lewisburg, Pennsylvania and reported in his research report entitled, "iPhone Applications & Privacy Issues: An Analysis of Application Transmission of iPhone Unique Device Identifiers (UDID's)" (last accessed December 19, 2010), online: http://www.pskl.us/wp/wpcontent/uploads/2010/09/iPhone-Applications-Privacy-Issues.pdf;

38. Further, the *Wall Street Journal*, as reported in the article "Your Apps Are Watching You," Scott Thurm and Yukari Iwatani Kane (December 18, 2010) independently confirmed that each non-Apple Defendant systematically uses its iPhone App to obtain iPhone users' UDID and location data and transmit it to multiple third parties.

39. None of the Defendants adequately informed Plaintiff and members of the proposed Class of their practices, and none of the Defendants obtained the consent of Plaintiff and members of the proposed Class to do so.

40. Apple's 159-page, single spaced terms of service states: "By using any location-based services on your iPhone, you agree and consent to Apple's and its partners and licensees' transmission, collection, maintenance, processing, and use of your location data to provide such products and services." The iPad terms of service is nearly identical.

41. The following Apps, however, do not provide location based services:

a. Paper Toss is a mobile device application owned by Defendant, Backflip Studios, Inc. Paper Toss is a gaming application that allows users to "throw" virtual paper balls into a digital wastebasket target. Paper Toss shares its UDID and/or users' Location (City, ZIP Code and Latitude/Longitude) with numerous third parties, including ad networks. No location based service is involved.

b. Pandora is a mobile device application owned by Defendant, Pandora Media, Inc. Pandora is a music application that allows users to access, stream and download digital music files. Pandora shares its users' UDID and Age, Gender, and/or Location (City, ZIP Code and DMA Code) with third parties, including ad networks. No location based service is involved.

42. There are simply no location based services involved in these Apps that would justify access to location data belonging to Plaintiff and members of the proposed Class. When this information is combined with UDID information belonging to Plaintiff and members of the proposed Class, it becomes personally identifying information. None of these Defendants adequately disclose to Plaintiff and members of the proposed Class that they are transmitting such information to third-party advertising networks.

43. In fact, prior to the *Wall Street Journal* report referenced above, the following Defendant did not have any privacy policy at all: BACKFLIP STUDIOS, INC. (Paper Toss App).

44. The UDID and location information obtained by each non-Apple Defendant was sent to multiple third-party advertising networks (in the case of Defendant Pandora, eight third parties).

45. As discussed above, Apple considers users' UDID information to be personally identifying information. By attempting to change its App Development criteria, Apple demonstrated that it is aware of the dangers posed by transmission of user data to third parties. Apple has simply failed to follow through on that conviction.

46. Plaintiff and members of the proposed class were harmed by Defendants' actions in that their personal, private information was obtained without their knowledge or consent.

Plaintiff and members of the proposed class were harmed in that their personal property – their computer – was hijacked by Defendants and turned into a device capable of spying on their every online move.

47. Valuable UDID information, demographic information, location information, as well as their application usage habits is a valuable commodity that Plaintiff and members of the proposed Class could have sold to research firms. Plaintiff and members of the proposed Class also consider this information to be personal and private. Such information was taken from them without their knowledge or consent. Plaintiff and members of the proposed Class should be compensated for this harm. Plaintiff and members of the proposed Class are entitled to compensation for this invasion of their privacy.

48. Each of the non-Apple Defendants is liable to Plaintiff and members of the proposed Class for violation of their statutory and common-law rights. Defendant Apple, by exercising significant control over App developers and sharing profits with them, has created a "community of interest" with the other Defendants to render them joint venturers, who are responsible for each other's torts. Defendant Apple has also aided and abetted the remaining Defendants in the commission of their legal wrongs against Plaintiff and members of the proposed Class. Based on the above, Apple has acted sufficiently in concert with the remaining Defendants to impose liability.

49. Plaintiff and members of the proposed Class bring this action to redress this illegal and intrusive scheme designed by Defendants to intrude into their personal lives and collect personal information about them.

50. Plaintiff and members of the proposed Class seek damages for their injuries, an injunction to protect those not yet harmed by these illegal activities, and, where legally available,

attorneys' fees and other costs associated with the bringing of this action.

Defendant Apple Aided and Abetted the Other Defendants

51. Defendant Apple knew or should have known the other Defendants' conduct constituted a breach of those Defendants' duties to Plaintiff and members of the proposedClass.

52. Defendant Apple gave substantial assistance to the other Defendants in committing the acts alleged in this Complaint. Furthermore, Apple had a duty to Plaintiff and members of the proposed Class to take steps to prevent such harm.

53. Such conduct by Apple constitutes Aiding and Abetting pursuant to New York State law and imposes liability on Defendant Apple for the other Defendant's torts, as outlined below.

Defendant Apple is in a Joint Venture with the Other Defendants

54. Defendant Apple's conduct and that of the remaining Defendants constitutes and undertaking by two or more persons jointly to carry out a single business enterprise for profit.

55. By reviewing each App, setting the conditions for and requirements for Apps to be sold and partnering with the above-named App developers in the sale of those Apps, Apple has created a "community of interest" in a common undertaking of which each partner has or exercises the right control and direction of the undertaking.

56. By sharing the profits of all App sales of the other Defendants' applications through the iTunes App Store, Apple is a joint venture with each of the remaining Defendants.

57. All members of a joint venture are jointly and severally liable for injuries resulting from the tortious conduct of one of the joint venturers, Apple is thus legally responsible for the tortuous conduct alleged in each of the Counts.

V. CLASS ACTION ALLEGATIONS

58. Pursuant to Fed. R. Civ. P. 23(b)(3), and 23(b)(2) Plaintiff brings this action on behalf of himself, and all others similarly situated, as representatives of the following class (the "Class"):

> Each and every individual in the United States of America who has placed on of Defendants' iPhone Apps or iPad Apps on their iPhone or iPad in the four years preceding the filing of this lawsuit (the "Class").
>
> Excluded from the Class are Defendants as well as all employees of this Court, including, but not limited to, Judges, Magistrate Judges, clerks and court staff and personnel of the United States District Courts for the Southern District of New York, the United States Court of Appeals for the Second Circuit and the United States Supreme Court; their spouses and any minor children living in their households and other persons within a third degree of relationship to any such Federal Judge; and finally, the entire jury venire called to for jury service in relation to this lawsuit. Also excluded from the class are any attorneys or other employees of any law firms hired, retained and/or appointed by or on behalf of the named Plaintiffs to represent the named Plaintiffs and any/or any proposed class members or proposed class in this lawsuit.
>
> Furthermore, to the extent that undersigned counsel has any legal interest to damages or other monetary relief, or other relief due to the putative class (or any other rights as potential putative class members), arising as a result of the causes of action asserted in this litigation, such interest is hereby disclaimed by undersigned counsel.

59. The requirements of Fed. R. Civ. P. 23 are met in this case. The Class, as defined, is so numerous that joinder of all members is impracticable. Although discovery will be necessary to establish the exact size of the class, it is likely, based on the nature of Defendants' businesses, that it numbers in the millions.

60. There are questions of fact and law common to the Class as defined, which common questions predominate over any questions affecting only individual members. The common questions include:

a. whether Defendants, as a regular practice, obtained and disseminated the Class' personally identifiable information without their knowledge and consent, or beyond the scope of their consent;

b. whether Defendants failed to disclose material terms regarding the collection and dissemination of the Class' personally identifiable information;

c. what use was made of the Class' personally identifiable information, including to whom the information was sold for a profit;

d. whether Defendants used iPhone Apps or iPad Apps to send UDID, location, and/or Username/password information belonging to Plaintiff and members of the proposed Class to third parties; and

e. whether personally identifiable information belonging to Plaintiff and members of the proposed Class was used to track his activity.

61. Plaintiff can and will fairly and adequately represent and protect the interests of the proposed Class as defined and have no interest that conflict with the interests of the proposed Class. This is so because:

a. All of the questions of law and fact regarding the liability of the Defendants are common to the Class and predominate over any individual issues that may exist, such that by prevailing on their own claims, Plaintiff will necessarily establish the liability of the Defendants to all members of the proposed Class;

b. Without the representation provided by Plaintiff, it is unlikely that any Class members would receive legal representation to obtain the remedies specified by relevant statutes and the common law;

c. Plaintiff has retained competent attorneys who are experienced in the conduct of

class actions. Plaintiff and his counsel have the necessary resources to adequately and vigorously litigate this class action, and Plaintiff and his counsel are aware of their fiduciary responsibility to the class members and are determined to diligently discharge those duties to obtain the best possible recovery for the Class.

62. Defendants' actions have affected numerous consumers in a similar way. The class action is superior to any other method for remedying Defendants' actions given that common questions of fact and law predominate. Class treatment is likewise indicated to ensure optimal compensation for the Class and limiting the expense and judicial resources associated with thousands of potential claims.

VI. CAUSES OF ACTION

COUNT I – COMPUTER FRAUD AND ABUSE ACT, 18 U.S.C. § 1030 (By Plaintiff And Members Of The Proposed Class Against All Defendants)

63. Plaintiff and members of the proposed Class incorporate by reference each proceeding and succeeding paragraph as though set forth fully at length herein.

64. By accessing and transmitting UDID and location data on the computer of Plaintiff and members of the proposed Class, Defendants have accessed Plaintiffs' computer, and those of the proposed Class, in the course of interstate commerce and/or communication, in excess of the authorization provided by Plaintiff and members of the proposed Class as described in 18 U.S.C. § 1030(a)(2)(C).

65. Defendants violated 18 U.S.C. § 1030(a)(2)(C) by intentionally accessing Plaintiff's computer, and those belonging to the members of the proposed Class, without authorization and/or by exceeding the scope of that authorization .

66. Plaintiff's computer, and those belonging to the members of the proposed Class, are protected computers pursuant to 18 U.S.C. § 1030(e)(2)(B).

67. Defendants thus further violated the Act by causing the transmission of a program, information, code or command and as result caused harm aggregating at least $5,000 in value.

68. Defendants' actions were knowing and/or reckless and, as outlined above, caused harm to Plaintiff and members of the proposed Class.

69. Plaintiff and members of the proposed Class seek recovery for this loss, as well as injunctive relief, to prevent future harm.

COUNT II – NEW YORK COMPUTER CRIME LAW NEW YORK PENAL CODE §§ 156, 156.05, 156.10, 156.20, 156.29, 156.30, AND 156.35 AND NEW YORK CRIMINAL PROCEDURE LAW §20.60 (By Plaintiff and Members of the Proposed Class Against All Defendants)

70. Plaintiff and members of the proposed Class incorporate the above allegations by reference as if set forth herein at length.

71. The New York Computer Crime Laws, regulate offenses involving computers, including but not limited to the unauthorized use of a computer, computer trespass, tampering, unlawful duplication of computer related material, and criminal possession of computer related material.

72. Defendants violated New York Computer Crime Law by knowingly accessing, copying, using, causing to be used, interfering, and/or altering, data belonging to Plaintiff and members of the proposed Class: (1) in and from the State of New York; (2) in the home states of the Plaintiff and members of the proposed Class; and (3) in the state in which the servers that provided the communication link between Plaintiff and members of the proposed Class and the websites they interacted with were located.

73. Pursuant to New York Computer Crime Law – Access means to instruct, communicate with, store data in, retrieve from, or otherwise make use of any resources of a

computer, physically, directly or by electronic means.

74. Pursuant to New York Computer Crime Law, computer data is property and means a representation of information, knowledge, facts, concepts, or instructions which are being processed, or have been processed in a computer and may be in any form, including magnetic storage media, punched cards, or stored internally in the memory of the computer.

75. Defendants have violated New York Computer Crime Law by knowingly using, causing to be used, and accessing, without permission, altering, and making use of data from Plaintiff's computer, and those belonging to the members of the proposed Class, in order to devise and execute business practices to deceive Plaintiff and members of the proposed Class into surrendering private electronic communications and activities for Defendants' financial gain, and to wrongfully obtain valuable private data from Plaintiff and members of the proposed Class.

76. Defendants have violated New York Computer Crime Law by knowingly accessing and without permission, taking, or making use of data from Plaintiff's computer, and those belonging to the members of the proposed Class.

77. Defendants have violated New York Computer Crime Law by knowingly and without permission, using and causing to be used Plaintiff's computer services, as well as those belonging to the members of the proposed Class.

78. Defendants have violated New York Computer Crime Law by knowingly and without permission providing, or assisting in providing, a means of accessing Plaintiff's computer, computer system, and/or computer network, as well as those belonging to the members of the proposed Class.

79. Defendants have violated New York Computer Crime Law by knowingly and

without permission accessing, or causing to be accessed, Plaintiff's computer, computer system, and/or computer network, as well as those belonging to the members of the proposed Class.

80. New York Criminal Procedure Law states: For purposes of bringing a civil or a criminal action under this section, a person who causes, by any means, the use of a computer or computer service in one jurisdiction from another jurisdiction is deemed to have personally used the computer or computer service in each jurisdiction.

81. Plaintiff and members of the proposed Class have also suffered irreparable injury from these unauthorized acts of disclosure, to wit: their personal, private, and sensitive electronic data was obtained and used by Defendants. Due to the continuing threat of such injury, Plaintiff and members of the proposed Class have no adequate remedy at law, entitling Plaintiff and members of the proposed Class to injunctive relief.

82. Plaintiff and members of the proposed Class have additionally suffered loss by reason of these violations, including, without limitation, violation of the right of privacy.

83. As a direct and proximate result of Defendants' unlawful conduct within the meaning of New York Computer Crime Law Defendants have caused loss to Plaintiff and members of the proposed Class in an amount to be proven at trial. Plaintiff and members of the proposed Class are also entitled to recover their Reasonable attorneys' fees pursuant to NY CPLR.

84. Plaintiff and members of the proposed Class seek compensatory damages, in an amount to be proven at trial, and injunctive or other equitable relief.

COUNT III – UNFAIR TRADE PRACTICES ACT
32 LAWS OF NEW YORK GENERAL BUSINESS LAW SEC. 349
(By Plaintiff and Members of the Proposed Class Against All Defendants)

85. Plaintiff and members of the proposed Class incorporate the above allegations by reference as if set forth herein at length.

86. In Violation of New York State General Business Law Section 349, Defendants engaged in consumer-orientated, commercial conduct described herein which was and is materially deceptive and misleading and caused injury to Plaintiff and members of the proposed Class.

87. Defendants' actions complained of herein occurred and continue to occur in the conduct of the defendants business or commerce or the sale of services.

88. Defendants' unconscionable and deceptive conduct occurred and continues to occur in the course of the defendants business and such conduct was part of a pattern or generalized course of repeated conduct on thousands of occasions. Defendants continue to engage in the acts complained of herein.

89. Defendants intended to and did deceive the Plaintiff and members of the proposed Class and its customers.

90. New York has enacted statutes to protect consumers from deceptive, fraudulent, and unconscionable trade and business practices such as those alleged in this complaint.

91. Defendants engaged in the deceptive acts and practices alleged herein in order to unjustly profit from consumers and represents unfair acts or practices that have the capacity to, and has and continues to deceive and injure consumers. The misrepresentations and omissions alleged herein were and are likely to mislead a reasonable consumer acting under the circumstances.

92. Absent some judicial intervention or relief, Defendants' conduct will continue to damage the consuming public.

93. As a direct and proximate result of the Defendants' violations of GBL §349 and other similar statutes, Plaintiff and members of the proposed Class have suffered damages. Plaintiff and members of the proposed Class are entitled to compensatory damages, equitable and declaratory relief, punitive damages, costs, and reasonable attorney's fees.

COUNT IV – TRESPASS TO PERSONAL PROPERTY
(By Plaintiff and Members of the Proposed Class Against All Defendants)

94. Plaintiff and members of the proposed Class incorporate by reference each proceeding and succeeding paragraph as though set forth fully at length herein.

95. By obtaining UDID and location data from Plaintiff's computer, and those belonging to members of the proposed Class, without their consent or knowledge, Defendants have improperly exercised dominion and control over personal property – their computer.

96. Defendants' actions were done knowingly and intentionally.

97. Defendants' actions caused harm to Plaintiff and members of the proposed Class, as described above.

98. Plaintiff and members of the proposed Class seek damages for this harm as well as injunctive relief to remedy this harm.

COUNT V – COMMON LAW CONVERSION
(By Plaintiff and Members of the Proposed Class Against All Defendants)

99. Plaintiff and members of the proposed Class incorporate the above allegations by reference as if set forth herein at length.

100. Defendants have taken Plaintiff's property, as well as property belonging to members of the proposed Class, in the form of information that is private and personal.

101. Plaintiff and members of the proposed Class have been harmed by this exercise of dominion and control over their information.

102. Plaintiff and members of the proposed Class bring this case seeking recovery for their damages and appropriate injunctive relief.

COUNT VI-UNJUST ENRICHMENT/ RESTITUTION
(By Plaintiff and Members of the Proposed Class Against All Defendants)

103. Plaintiff and members of the proposed Class incorporate the above allegations by reference as if set forth herein at length.

104. Defendants have improperly and illegally profited from the obtainment and/or sale of personal, private data belonging to Plaintiff and members of the proposed Class. Defendants' actions have been done knowingly and secretively with the intent that Plaintiff and members of the proposed Class not realize what was being done.

105. These actions constitute violations of both statutory as well as common law obligations as outlined above.

106. Under the principles of equity and good conscience, Defendants should not be permitted to retain the benefits they have acquired through this unlawful conduct. All funds, revenues and benefits that Defendants have unjustly received as a result of their actions rightfully belong to Plaintiff and members of the proposed Class.

WHEREFORE, Plaintiff and members of the proposed Class demand judgment on their behalf to the following effect:

a. declaring that this action may be maintained as a class action;

b. granting judgment in favor of Plaintiff and members of the proposed Class against the Defendants;

c. treble and/or punitive damages should the Court find that the Defendants acted in willful or reckless disregard of the law;

d. declarations that Defendants' acts and practices alleged herein are wrongful;

e. an order directing restitution or disgorgement in an allowable amount to be proven at trial;

f. compensatory damages in an amount to be proved at trial;

g. pre and post judgment interest to the maxim extent permissible;

h. an award to Plaintiff and members of the proposed Class of their costs and expenses incurred in this action, including reasonable attorneys' fees, to the extent permissible;

i. injunctive relief preventing Defendant from further collecting and disseminating the personally identifiable information belonging to Plaintiff and members of the proposed Class and/or requiring more detailed disclosure and informed consent regarding this activity; and

j. such other relief as the Court deems appropriate.

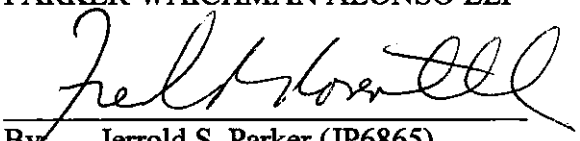
DEMAND FOR JURY TRIAL

Plaintiff and members of the proposed Class demand a trial by jury of all issues so triable.

Dated: Port Washington, New York
April 27, 2011

RESPECTFULLY SUBMITTED,

PARKER WAICHMAN ALONSO LLP



By: Jerrold S. Parker (JP6865)
Fred R. Rosenthal (FRR4528)
6 Harbor Park Drive
Port Washington, New York 11050
Telephone: (516) 466-6500
Facsimile: (516) 466-6665
Email: jerry@yourlawyer.com
frosenthal@yourlawyer.com